CIBERCRIME: UM ESTUDO ACERCA DO CONCEITO DE CRIMES INFORMÁTICOS

CYBERCRIME: A STUDY OF THE CONCEPT OF COMPUTER CRIMES

Júlio César ALEXANDRE JÚNIOR[1]

ISSUE DOI: 10.21207/1983.4225.602

RESUMO

A presente pesquisa visa discorrer acerca do conceito de crimes cibernéticos ou cibercrimes sob o viés do Código Penal Brasileiro. Denomina-se cibercrimes os crimes que são praticados por meio cibernéticos, ou seja, atividades que envolvam a prática ilícita por meio de um computador na rede informacional de comunicação tecnológica. Cibercrime está associado ao "fenómeno da criminalidade informática estão, sem dúvida, condutas violadoras de direitos fundamentais, seja através da utilização da informática para a prática de um crime, ou como um elemento do tipo legal de crime" (SIMAS, 2014, p. 12). O Brasil está intrinsicamente ligado neste novo contexto de crimes praticados por meio de tecnologias informacionais de comunicação, ora, como exemplo, à comunidade internacional em ações que visam o combate desse delito, ora como foco irradiador e proliferador de ações criminosas cibernéticas. Diante do exposto, esta pesquisa apresentará o conceito de cibercrime e debruçará, não de modo exaustivo, sobre o cibercrime em âmbito internacional e nacional, bem como, um estudo acerca do Tratado de Budapeste, o qual dimensiona a Lei ao combate de crimes praticados por meio de sistemas informáticos, e da Lei n. 12.737/2012.

Palavras-chave: Cibercrime; Código Penal Brasileiro; Crimes Eletrônicos.

ABSTRACT

The present aims to discuss about the concept of cybercrime or cybercrime under the bias of the Brazilian Penal Code. It is called cybercrime the crimes that are practiced through cybernetics, that is,

[1] Possui graduação em Letras Vernáculas e Clássicas - Habilitação: Licenciatura em Língua Portuguesa e Respectivas Literaturas pela Universidade Estadual de Londrina – UEL (2011). Possui Especialização em Literatura Brasileira pela Universidade Estadual de Londrina – UEL (2014). Atualmente, é graduando do Curso de Direito pela Universidade Norte do Paraná – UNOPAR, do Curso de Licenciatura em Letras Português e Inglês pela Universidade Cruzeiro de Sul – UNICSUL e pós-graduando em Língua Portuguesa pela Faculdade de Educação São Luís – FESL. Contato: julio_cajr@hotmail.com. http://lattes.cnpq.br/2092321905177013.

activities that involve illicit practice through a computer in the informational network of technological communication. Cybercrime is associated with "the phenomenon of computer crime are undoubtedly conduct that violates fundamental rights, either through the use of information technology to commit a crime, or as an element of the legal type of crime" (SIMAS, 2014, p. 12). Brazil is intrinsically connected in this new context of crimes practiced through informational communication technologies, or as an example, to the international community in actions that aim to combat this crime, or as an irradiating and proliferating focus of cybernetic criminal actions. In view of the above, this research will present the concept of cybercrime and will not exhaustively address cybercrime at the international and national levels, as well as a study on the Budapest Treaty, which stipulates the Law to combat crimes committed by Computer systems, and Law n. 12.737/2012.

Keywords: *Cybercrime; Brazilian Penal Code; Electronic Crimes.*

1 INTRODUÇÃO

Atualmente, não se pode contestar o papel que as novas tecnologias de informação e comunicação, a Internet, tem proporcionado à vida dos cidadãos, seja em meio social, cultural, econômico. Os meios de tecnologias informacionais de comunicação tornam-se (e tornaram-se) elementos essenciais à atividade humana para o seu desenvolvimento.

Em meio à Era da Informação, com o desenvolvimento tecnológico, a sociedade tornou-se, transformou-se em uma sociedade global, proporcionando meios positivos, oportunidades para o indivíduo. No entanto, com a evolução da tecnologia informacional, também apresentou riscos a partir de sujeitos que as utilizam em condutas ilícitas, as quais passaram a serem praticadas nesse novo ambiente. Esta conduta ilícita passou a ser denominada como *cibercrime*.

A partir da evolução tecnológica, facilitadora para os cidadãos, seja pessoal, laboral ou social, notadamente, a liberdade de circulação na Internet deveria ser aliada a direitos que pudessem garantir a segurança aos indivíduos que usufruem (ou não) dessa tecnologia. No entanto, com grandes vantagens que o meio informático, informacional e tecnológicos, há também as desvantagens, as condutas ilícitas, os desvencilhamos nocivos à pessoa e dignidade humana.

As condutas, a partir do cibercrime, revelaram uma nova ameaça à medida que conceitos tradicionalistas – jurisprudências, competências e soberanias – precisaram e precisam ser interpretadas sob ótica atual, por meio das relações de criminalidade. A partir da Internet, este instrumento apresentou facilidades às práticas de fatos para o crime, seja ele tradicional ou com outra denominação de crime.

De acordo com artigo publicado pelo Jornal *El País* em 22 de outubro de 2015, intitulado *O problema do cibercrime no Brasil*, o Brasil está entre os principais centros de criminalidade praticados em meios cibernéticos ou cibercrimes. O nosso País está em segundo lugar na classificação mundial de fraudes bancárias *online* e *malware* financeiro, o que é um dado alarmante para os dias atuais. De acordo com a publicação do renomado Jornal, o número de ataques cibernéticos no Brasil cresceu, assustadoramente, em 197% (cento e noventa e sete por cento) em 2014, e as fraudes bancárias *online*, 40% (quarenta por cento).

O Brasil está intrinsicamente ligado neste novo contexto de crimes praticados por meio de tecnologias informacionais de comunicação, ora, como exemplo, à comunidade internacional em ações que visam o combate desse delito, ora como foco irradiador e proliferador de ações criminosas cibernéticas.

Diante do exposto, esta pesquisa apresentará o conceito de cibercrime e debruçará, não de modo exaustivo, sobre o cibercrime em âmbito internacional e nacional, bem como, um estudo acerca do Tratado de Budapeste, o qual dimensiona a Lei ao combate de crimes praticados por meio de sistemas informáticos, e da Lei n. 12.737/2012.

2 O QUE É CIBERCRIME?

O *cibercrime* nada mais é que todo ato em que o computador ou meios de tecnologia de informação serve para atingir um ato criminoso ou em que o computador ou meios de tecnologia de informação é objeto de um crime. O cibercrime está associado ao fenômeno da criminalidade informacional de condutas violadoras de direitos fundamentais, seja por meio da utilização da informática para a prática do crime ou como elemento de tipo legal de crime.

Em sentido amplo, a criminalidade informática engloba toda atividade criminosa realizada por computadores ou meios de tecnologia da informação. Em sentido *stricto*, a criminalidade informação engloba crimes, de acordo com Simas (2014, p. 12), "quem que o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital".

Como referimos no início deste trabalho, a informática pode ser um instrumento de práticas de crimes tradicionais, isto é, que não necessitam de suporte informacional para serem realizados, nem sendo parte legal. A este disso, podemos citar crimes cometidos a honra e a dignidade da pessoa humana, que podem ser cometidos com recurso em meio informático para divulgação (e-mail, redes sociais). Outros casos que podemos inferir são quando a informática surge como elemento integrador, isto é, podendo o bem jurídico protegido não ser excepcionalmente com a informática, como é o caso de crimes contra *softwares* em que o bem jurídico protegido é autoral.

A doutrina brasileira, por meio da Lei n. 12.737, de 30 de novembro de 2012, a qual dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências, especifica, em seu Art. 154-A, os crimes cometidos por meios informacionais:

> Art. 154-A. Invadir disposto informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismos de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" (BRASIL, 2012, s.p.).

A nossa doutrina penal estabelece pena de detenção de 3(três) meses a 1(um) ano e multa. Além disso, a referida Lei adverte que a pena incorre quem produz, oferece, distribui, vende ou difunde dispositivos ou programas de computadores que tem por objetivo permitir a prática da conduta criminosa; se resulta em prejuízo econômico; e, se da invasão resulta obtenção do conteúdo. A pena de reclusão repercute em 6(seis) meses a 2(dois) anos e multa, caso a conduta criminosa tornar-se grave. Ainda, aumenta-se a pena se atingir ou praticar contra a Administração Pública municipal, estadual ou federal.

A prática de crimes realizados via internet assume outras denominações, que são: crime digital, crime informático, crime informático-digital, *high technology crimes*, *computer related crime*, dentre outros. Todavia, consideraremos o interesse em utilizar o termo *cibercrime* nesta pesquisa.

3 A INTERNET E O CIBERCRIME

A internet foi criada no final da década de 1960, cujo principal intuito foi a partir de objetivo militares. O termo "Internet" surgiu décadas depois, quando a "nova" tecnologia passou a ser utilizada com o objetivo de ligar universidades americanas entre si e, logo em seguida, institutos de pesquisa sediados em outros países. A exploração mercadológica iniciou na década de 1990 e desenvolveu o serviço de *World Wide Web*, sendo um pacote de informações em formato de texto, mídia (imagens, áudios e vídeos), organizadas para um indivíduo percorrer em dezenas de páginas da rede.

Atualmente, percebe-se que a Internet desempenha um papel significativo na sociedade, servindo de suporte para o governo, segurança, economia, telecomunicação, transporte, educação energia, saúde e estendendo-se a todo tipo de relação, seja comercial, cultural, social e pessoal. Com a dependência da sociedade pela tecnologia informacional, o cibercrime tornou-se um fenômeno crescente e frequente, internacionalmente, para criminosos, violando os direitos fundamentais.

De acordo com Simas,

> A evolução operada nas novas tecnologias, projectou-se sobre o fenómeno criminal, pois se atendermos às suas duas vertentes, por um lado, a tecnologia poder, ela mesma, objecto de prática de crimes e por outro lado, suscita e potencia novas formas criminais ou novas formas de praticas antigos crimes (SIMAS, 2014, p. 14).

Evidencia-se, portanto, que, para o problema da prática cibernética, impõe-se nível de segurança, fiabilidade e eficiência no âmbito da Internet, criando sistemas de segurança de rede.

4 O CIBERCRIME EM ÂMBITO MUNDIAL E NACIONAL

4.1 A CONVENÇÃO DE BUDAPESTE

Criada no início da década de 2000 pelo Conselho da Europeu, na Hungria, a Convenção de Budapeste foi promulgada apenas em 2004,

após a retificação de cinco países. Atualmente, engloba 20 países europeus e o seu principal objetivo é tipificar os principais cometidos na Internet.

Em seu preambulo, a Convenção de Budapeste prioriza "uma política comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional" (CONVENÇÃO DE BUDAPESTE, 2001). O referido Tratado possui quatro capítulos, que são: Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais, respectivamente, e 48(quarenta e oito) artigos.

O principal destaque do Tratado é a definição de cibercrime (Capítulo I), tipificando-os como infrações contra sistemas e dados de tecnologias da informação (Capítulo II, Título I), infrações relacionadas com computadores (Capítulo II, Título II), infrações relacionadas com o conteúdo, pornografia infantil (Capítulo II, Título III), infrações relacionadas com a violação e direitos autorais (Capítulo II, Título IV), cujas proposituras estão adentradas em Direito Penal Material.

Quando trata-se de matérias acerca do Direito Processual Penal, o Tratado dispõe de, segundo Souza e Pereira (2009, p. 5),

> [...] âmbito das disposições processuais, condições e salvaguardas, conservação expedita de dados informáticos armazenados, injunção, busca e apreensão de dados informáticos armazenados, recolha em tempo real de dados informáticos e interceptação de dados relativos ao conteúdo.

Em Art. 1º, define-se a Convenção consistente a um sistema informático, dados informatizados, fornecedor de serviços e dados de trafego, sendo este conferido a parte no tocante à proteção jurídica a ser atribuída, consoante a realidade do país que adere ao Tratado.

A Convenção teve por objetivo criar normas comuns, não excluindo a possibilidade de cada membro do Tratado adequar à sua legislação nacional, podendo excluir infrações de menor punibilidade de aplicação dos Arts. 2º ao 10º, bem como, formular reservas de determinadas circunstâncias – Arts. 40 e 42.

Os crimes previstos pela Convenção de Budapeste são acometidos de forma dolosa para que seja imputada a responsabilidade criminal, sendo que, em casos específicos, é exigido uma intenção e soma específica, como estabelecido no Art. 8º: Fraude relacionada com computadores.

4.2 DIREITO PENAL MATERIAL

O Capítulo ao qual refere-se o Direito Penal Substantivo – Arts 2º ao 13 – define 9(nove) crimes agrupados em 4(quatro) categorias distintas, seguidos pela responsabilidade acessória e respectivas sanções. De acordo com o Tratado de Budapeste, são considerados crimes cibernéticos, sendo que cada Parte deverá adotar as medidas legislativas e outras que se revelem necessárias para classificação da infração penal nos termos:

a) Acesso ilícito (Art. 2º): da prática intencional de acesso ilícito a um sistema informático ou parte dele;
b) Intercepção ilícita (Art. 3º): da prática intencional a interceptação não autorizada;
c) Dano provocado nos dados (Art. 4º): da prática intencional à danificação, a exclusão de dados, a deterioração, a alteração ou supressão não autorizada de dados;
d) Sabotagem informática (Art. 5º): da prática intencional, a perturbação grave e não autorização quando do funcionamento de um sistema informático mediante inserção, transmissão, danificação, eliminação, deterioração, alteração ou supressão de dados;
e) Utilização indevida do dispositivo (Art. 6º): da prática intencional e ilícita, a saber: produção, venda, aquisição para efeitos de utilização, importação, distribuição e suas outras formas e estar em possa de material criminoso;
f) Falsificação informática (Art. 7º): da prática intencional e ilícita, a introdução, a alteração, a exclusão ou a supressão de dados dos quais não resultem em autenticidade;
g) Burla informática (Art. 8º): da prática intencional e ilícita, prejuízo patrimonial causado a outrem por meio de qualquer introdução, alteração, exclusão ou supressão de dados, bem como, qualquer interferência nas funções de um sistema informático com a intenção de benefício econômico;
h) Infrações relacionadas com pornografia infantil (Art. 9º): quando da prática de forma intencional e ilegítima por meio de um sistema informático: produção, oferta, disponibilização, difusão, posse e deverá abranger a todos os menores de 18(dezoito) anos de idade; e
i) Infrações relacionadas a violação de direitos autorais e conexos (Art. 10º).

O artigo 11 da Convenção de Budapeste impõe aos Estados membros que adotem medidas para classificação das infrações penais, nos termos da Lei interna, com auxílio ou a instigação à prática de qualquer infração prevista nos Arts. 2º ao 10º. Relacionado ao Art. 12, é previsto como

responsabilidade penal das pessoas coletivas. Já o Art. 13, dispõe das sanções e medidas as quais obriga a cada Estado membro a punir com sanções eficazes, proporcionais e dissuasivas os crimes praticas por meio de um sistema informático.

A Convenção ainda relacionou os tipos de crimes em distintos títulos, a saber:

a) Título I: crimes relacionados com computadores, crimes que atentam a confiabilidade, a integridade e disponibilidade de sistemas e dados informatizados (Arts. 2º ao 6º);
b) Título II: outros crimes relacionados com computadores (Arts. 7º e 8º);
c) Título III: crimes relacionados ao conteúdo, como produção ou distribuição ilícita de pornografia infantil (Art. 9º);
d) Título IV: crimes relacionados com a violação de direitos autorais e conexos (Art. 10º); e
e) Título V: disposições acerca da tentativa, auxílio e cumplicidade, sanções e medidas (Arts 11 ao 13).

4.3 DIREITO PROCESSUAL PENAL

As medidas referentes ao direito processual penal de acordo com a Convenção possuem por espoco a facilitação e promoção à uma melhor investigação criminosa por meio de materiais informáticos, relativamente às infrações constantes do direito penal substantivo, mas, sobretudo a outras cometidas por meio do mesmo sistema e recolhimento de provas.

Podemos, portanto, considerar que, a nível nacional, os Estados membros à Convenção adotarão medidas de direito processual que se apliquem a: crimes previstos no Capítulo II, seção I; crimes cometidos por meio de um sistema informático; e o recolhimento de provas eletrônicas. Os procedimentos que abrangem o tipo de dados informáticos são: dados de tráfego, conteúdo e subscritores, os quais são divididos em armazenados e presentes no processo de comunicação.

Quando tratados de Direito Processual, cuja Convenção se faz referência, aplica-se a qualquer infração cometida por meio informático ou prova eletrônica, adotando meio de obtenção como a busca e apreensão dos materiais informáticos, cuja determinação às condições de aplicabilidade processual são:

a) Preservação e conservação expedita de dados informatizados de armazenamento (Art. 16);
b) Preservação e conservação expedita e divulgação parcial de dados de tráfego (Art. 17);
c) Injunção de comunicar e ordem de produção (Art. 18);
d) Investigação e apreensão de dados informatizados (Art. 19);
e) Recolhimento de dados de tráfego em tempo real (Art. 20);
f) Interceptação de dados de conteúdo (Art. 21);
g) Jurisdição (Art. 22).

Por fim, a Convenção de Budapeste preocupe-se com a cooperação internacional, prevendo, de acordo com o Capítulo III, a assistência mútua para casos de crimes tradicionais e cibercrimes, assim como, relacionado a extradição criminal. Quando se regula a assistência mútua a crimes tradicionais, não existindo uma base jurídica, aplica-se as medidas e sanções da Convenção. Outro lado, quando houver uma base jurídica, aplica-se à assistência prestada ao abrigo da Convenção.

5 LEI N. 12.737/2012

A Lei que faz a apresentação deste do Diploma Penal faz-se legal, de modo que buscou-se manter o ideal de que os delitos informáticos não se afastam sobremaneira da realidade material, podendo ser sancionados, reprimidos de acordo com a legislação vigente.

A descrição da Lei n. 12.737/2012 como tipificação criminal de delitos informáticos vem a englobar os crimes praticados por meio de sistemas informáticos. A referida Lei foi sancionada com o objetivo de combater as práticas danosas causando transtornos àqueles que utilizam ou dependem de meios informáticos para o lazer, o trabalho. Conforme o Art. 154-A, explanado pela Lei de Cibercrimes é combater a invasão de dispositivo informático alheio, conectado ou não a rede informática. Criminaliza-se, outrossim, a invasão, o acesso sem permissão aos conteúdos armazenados em dispositivos informáticos.

A Lei prevê que a ação de acessos ilícitos seja realizada mediante a violação de mecanismos de segurança, o que corresponde, em outros casos, a sistemas antivirais, com o intuito de proteção ao sistema informático. Contudo, também, corresponde a obrigação de preencher senhas de acesso à internet, banco de dados e demais funcionalidades informatizadas. Para

Oliveira (2013), verifica-se uma falha na lei, pois "no *caput* do artigo acaba por condicionar a invasão do dispositivo a uma violação de mecanismo de segurança" (OLIVEIRA, 2013, p. 43).

A condutada tipificada no *caput* do Art. 154-A pode ser realizada, praticada, por qualquer indivíduo que queira praticar uma intenção delituosa informática. Não é preciso qualquer qualidade especial para intentá-la, caracterizando um crime comum. Da mesma forma, qualquer indivíduo pode ser alvo – sujeito passivo do crime –, tornando-o comum a prática criminosa.

Vale lembrar que o Brasil não é um Estado membro do Tratado de Budapeste, pois apresenta-se com lei própria, ainda frágil diante da realidade que a sociedade vive. A criação da Lei, alterando artigos do Código Penal, o qual necessita de uma revisão, dado a sua promulgação secular passada, teve o condão de preencher o vazio normativo existente na legislação penal do Brasil, o qual permitia a prática de atos ilícitos informáticos, ante a ausência da tipificação.

6 CONSIDERAÇÕES FINAIS

O avanço consta das tecnologias de informação tem um impacto significativo na sociedade atual. As evoluções tecnológicas não trouxeram apenas aspectos positivos, pois, como pode-se verificar no decorrer dessa pesquisa, alguns indivíduos têm usado sistemas informáticos com o intuito de invadir a privacidade alheia, vender, distribuir materiais de cunho ilícito. Para tanto, a troca de informações e conhecimentos de forma facilitada e simples, permitiu também o surgimento de práticas tidas delituosas.

Com o surgimento de novas práticas criminosas por meio de sistemas informáticos, permitiram novos crimes associados às novas tecnologias, como a prática de crimes tidos como clássicos. Os *cibercriminosos* encontra-se muitas vezes em locais distintos, dificultando a sua localização. Conforme Simas (2014, p. 163),

> O carácter transfronteiriço destas infracções entra em conflito com a territorialidade das autoridades nacionais competentes para a aplicação da lei. As legislações nacionais estão confinadas a um território delimitado, pelo que se torna cada vez mais importante que exista legislação internacional.

Faz-se necessária esta pesquisa para o Direito Brasileira face que os crimes praticados por meio de equipamentos informáticos, tradicionais ou não, estão em conflito com a competência e atuação territorial das autoridades nacionais, uma vez que as leis têm aplicação limitada. Portanto, faz-se necessária a participação do Brasil no Tratado de Budapeste para que crimes cibernéticos internacionais contra o nosso País sejam solucionados. Corroborando com Simas (2014), tornou-se necessária a aplicabilidade de medidas de caráter técnico – nacional e internacional – em conjunto com medidas jurídicas com o intuito de evitar e deter a prática de crimes.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Lei n. 12.735, de 30 de novembro de 2012.** Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei n. 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistemas eletrônicos, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outas providências. Acesso em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm

_____. **Lei n. 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Acesso em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

CONVENÇÃO DE BUDAPESTE. **Convenção sobre o Cibercrime.** 2001. Acesso, em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf

MUGGAH, Robert. O problema do cibercrime no Brasil: está na hora de os legisladores brasileiros começarem a levar a sério o crime cibernético. In: **El País.** Acesso em: https://brasil.elpais.com/brasil/2015/10/23/opinion/1445558339_082466.html

OLIVEIRA, J. C. **O cibercrime e as Leis n. 12.735 e 12.737/2012.** 2013. 61f. Trabalho de Conclusão de Curso (Graduação em Direito). Departamento de Direito. Universidade Federal de Sergipe. São Cristóvão. 2013.

SIMAS, Diana Viveiros de. **O cibercrime.** 2014. 168f. Dissertação (Mestrado em Ciências Jurídico-Forenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa. 2014.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. A convenção de Budapeste e a leis brasileiras. In: **Anais do 1º Seminário "Cibercrime e Cooperação Penal Internacional"**. Org. CCJ-UFPB e *Association Internacionale de Lutte Contra la Cybercriminalite* (França), João Pessoa/PB, maio de 2009. Acesso em: http://www.egov.ufsc.br/portal/conteudo/conven%C3%A7%C3%A3o-de-budapeste-e-leis-brasileiras.